IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.
Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Trust aware secure energy efficient hybrid Protocol for MANET

Neenavath Veeraiah[1],Osamah Ibrahim Khalaf[2], C.V.P.R.Prasad[3],Youseef Alotaibi[4] ,Abdulmajeed Alsufyani[5] , Saleh Alghamdi[6] , Nawal Alsufyani[7]

[1]Department of Electronics and Communications, DVR&DHS MIC Engineering College, Kanchikacharla, Vijayawada, A.P,India.
[2]Al-Nahrain University, Al-Nahrain Nanorenewable Energy Research Center,Baghdad,Iraq.
[3]Professor and Head, Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Hyderabad, T.S, India.
[4]Department of Computer Science, College of Computers and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia.
[5]Department of Computer Science, College of Computers and Information Technology, Taif University, P.O.Box. 11099, Taif 21944, Saudi Arabia.
[6]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia.
[7]Department of Computer Science, College of Computers and Information Technology, Taif University, P.O.Box. 11099, Taif 21944, Saudi Arabia.

Corresponding author: Neenavath Veeraiah (e-mail: neenavathveeru@gmail.com).

We deeply acknowledge Taif University for Supporting this study through Taif University Researchers Supporting Project number (TURSP-2020/115), Taif University, Taif, Saudi Arabia.

ABSTRACT Mobile ad hoc network (MANETs) is infrastructure-less, self-organizing, fast deployable wireless network, so they truly are exceptionally appropriate for purposes between special outside occasions, communications in locations without a radio infrastructure, crises, and natural disasters, along with military surgeries. Security could be the primary weak spot in manet on account of this flexibility of structures and always changing dynamic topology, that will be very exposed to your selection of strikes like eavesdropping, routing, and alteration of programs. MANET is affected with security issues, surpassing Quality of services (QoS).So, intrusion tracking which modulates your system to recognize some other violation weakness would be that the top approach to guarantee security for MANET. Detecting intrusions has a critical part in supplying protections and functions as beyond layer of defenses against access. Power collapse of the cellular node maybe not merely alter the node alone but its capacity to forwards packets which is based on total system life. This also caused the institution of the routing protocol to its stable optimal choice of this multi-path to increase the navigation MANETs. Provision of energy-efficient and secure routing is a challenge given the changing topology and restricted resources of this kind of network. To address the energy efficiency and security we suggest a trust-based secure energy efficient navigation in MANETs employing the hybrid algorithm, cat slap single-player algorithm (C-SSA), that selects the best jumps in advancing the routing. In the beginning, the fuzzy clustering is put on, and the cluster heads (CHs) are picked predicated maximum worth of indirect, direct, and recent trust. Predicated on trust threshold worth nodes additionally discovered. Even the CHs are participated from the multi hop routing, and the assortment of the best route relies upon the projected hybrid protocol, and that selects the best routes determined by the delay, throughput, along with connectivity within this course. The proposed method obtained a minimal energy of 0.11m joules, a negligible delay of 0.005 msec, a maximum throughput of 0.74 bps, a maximum packet delivery ratio of 0.99 percent, and a maximum detection rate of 90%. The proposed method compared with the existing techniques in the presence and absent of the selective packet dropping attack.

INDEX TERMS MANET, Selective packet dropping attack, Energy efficiency, Cluster head, Trust values.

I. INTRODUCTION

Mobile Ad hoc Network (MANET)[1] includes nodes equipped using a radio broadcaster along with also a receiver which works from the system via bidirectional wireless connectivity. The essential benefits of why MANETs are allowing data-transmission within comparable possessions and maintaining their energetic methodology [2, 3]. Oddly, this transmission is more confined to this transmission scope, so any number of nodes find it impossible to swap data over the system [4]. Energy Efficiency can be a significant problem of problem in wi-fi that an ad hoc network since portable nodes be dependent upon batteries, and that can be confined resources of vitality, also in most surroundings, it is very a cumbersome endeavor to recharge or replace them. Despite the advancements made in battery life technology, the life of battery powered device has been function as vital challenge also necessitates added exploration on productive design and style of protocols, platforms, and technologies. Considering those power resources have a minimal life, ability accessibility is just one among the main limitations for its performance of their ad hoc system.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3108807, IEEE Access

Conversation is just one among the primary origins of electricity ingestion. Due to the fact the pace of battery life operation advancement is quite slow now, also at the lack of discoveries within this discipline, additional measured must be required to reach the target to gaining much more effectiveness out from their now readily available battery life resources. The vitality consumption which has been identified dependent on delivering packet, though using a package, whilst at idle manner and in sleeping manner that takes place whenever the wireless port of the cell node has been deterred. Devices utilized in the cellular ad hoc systems call for portability as they have been portable, additionally they have weight and size limitations together side the limitations about the ability resource. In case the battery is raised, it can create the nodescumbersome and not as mobile. Thus, the vitality efficacy stays an essential design factor for MANETs.

MANETs Are exposed to several kinds of risks like some other radio-based media technologies. These dangers comprise outdoors attackers in addition to misbehaving things onto the interior. Hence, a number of information pledge technologies will need to get implemented to guard these sorts of systems, like data protection, access management, identification administration, and intrusion detection. Alas, several of the well-established intrusion-detection procedures and implementations aren't instantly invisibly from infrastructure-based IP address networks, as you'll find lots of intensive implications regarding the using wireless connections and also the freedom of their various apparatus. Maybe not merely contains got the strike for smart and broadband continues to be expanded, however, also the chance of impersonation and Man in the Middle strikes while in the system has additionally grown. As a result of chance of ineffective transport of protocol packs, the likelihood of false alerts and untrue accusations of nodes from the networks is quite important. This potential improves with bodily motion while in the system that causes disruption of broadcasts and lots of paths. Moreover, There Aren't Any Essential places from the system, in which all Appropriate visitors Could Possibly Be detected and examined so as to discover malicious behavior, that has been true such as switches, routers, and firewalls in wired IP networks

The objective of the work is to provide the secure and energy efficiency routing protocol for MANETs by utilizing a hybrid algorithm. In the beginning, the fuzzy clustering is put on, and the cluster heads (CHs) are picked predicated maximum worth of indirect, direct, and recent trust. Predicated on trust threshold worth nodes additionally discovered. Even the CHs are participated from the multi hop routing, and the assortment of the best route relies upon the projected hybrid protocol, and that selects the best routes determined by calculating the fitness function of the route. The fitness function is the the sum of energy left in the nodes, the path's throughput, and the path's accessibility or connectivity. At step one,the CHs from the MANETS natural environment is decided on dependent upon the Fuzzy Clustering [5] with maximum worth of indirect, direct and the recent hope, that will be followed closely by intrusion detection procedure for discovering intruded node for stable transmission of their packets from origin to destination together with all the productive routing together with an hybridization algorithm that's accessed from the integration of this salp swarm optimization (SSA) and cat salp optimization (CSO)algorithm after the purpose functionality. The supposed purpose function relies on the ability, throughput, and connectivity within this trail. The suggested hybrid algorithm features the benefits of the SSA and CSO algorithms, and there's a productive tradeoff between both mining and manipulation stages of this algorithm that is projected. The simulation results will be examined dependent on discerning packet falling strike

The organization of this paper is the following: Section II discusses the motivation with literature inspection of this existing techniques. The suggested way of routing is shown in section III, also and section IV acknowledges that the effective method. Finally, the outline is supplied in section V

II. MOTIVATION

In this part, the literature evaluation is provided with the requirement to create a procedure. The difficulties of several techniques remain at the conclusion of this section, which motivates research into a trust aware fuzzy clustering with multi-objective (fitness factors) optimization algorithm for the MANET.

A) LITERATURE REVIEW

With MANETs, a mobile node's limited battery capacity impacts network survival, because when the battery is depleted connection is severed. A routing technique that considers mobile nodes energy is thus necessary to ensure a network Connectivity and extend the lifespan of the network. Security is a significant issue. Various security problems such as node authentication and creation of trust, key agreement and detections are observed. In recent years, several routing techniques have been created to improve the lifespan of a route and the network in turn. Multipath routing protocols are one of these breakthroughs. Multilateral routing systems allow the source node to choose the optimal route amongst multiple routes in a single route discovery procedure. For this concerned we summarize the following papers.

Veeraiah, N., Krishna, B.T[6] suggests, based on an optimization algorithm, a powerful multipath routing protocol in MANET. The MANET energy and protection crisis is efficiently tackled using the collection and intrusionmitigation techniques of the cluster head (CH), including fuzzy clustering and fuzzy Naive Bayes (fuzzy NB). The multipath routing is then progressed using the Bird Swarm- Whale Optimization Algorithm (BSWOA), which is the incorporation of bird swarm optimization (BSA) into the whale optimization algorithm, based on the routing protocol(WOA). Prasad P, R, Shankar [7] suggested EA-DRP protocol was implemented with modifications to the current DSR and total energy

consumption in the proposed protocol was reduced. An improvement in energy management may thus be seen owing to the change and now consideration of the efficient energy protocol in the area of MANETs. The EA-DRP algorithm averages the energy reduction of the network to a high level, as demonstrated in the simulation results. The EA-DRP adopted has minimal energy consumption in order to enhance network communication and to find road routes between mobile nodes in the network. This method performance is low for different types of attacks. S. Vinod Kumar, Dr. V. Anuratha [8] suggested Energy Efficient EE-OHRA route discovery for mobile ad hoc networks is a version intended to address issues related to reducing energy consumption and maximizing course life. When our suggested course discovery method regards the life of the course since the metric is reduced as the route is chosen. This lowers the diversity of routing discovery methods as well as the overhead calculation of all nodes involved, which influence the overall speed of the routing protocol. This method performance is also low for different types of attacks. S. and R. Jain. K. Sharma [9] The suggested solution requires an adaptive strategy in which the energy performance of our proposed scheme is greater. The filtering forwarding scheme slows down the spread of excessive RREQs generated per unit time by a node and prevents. Denial of Service attacks with success. This paper envisaged multipath extensions and a security enhancement toward the AODV routing protocol. The hash function with location update algorithm is proposed in the Ad hoc On-Demand Distance Vector (AODV) routing protocol to boost protection against selfish nodes in Mallikarjun Anantapur, VenkanagoudaChanabasavanagouda Patil [10]. To relay the data packets from the source to the destination, the AODV routing protocol is used. Therefore, to reduce packet loss across the network, the Prevention of Selfish Node utilizing Hash Function (PSNHF) with location update algorithm is suggested. A revolutionary Quality of Service based protected multi-path routing scheme is proposed for efficient data communication along with encryption technique. Rajashanthi, M., Valarmathi, K. [11] The AODV-BR protocol with Optimal Fuzzy Logic is also built for the multipath routing phase. The Grey Wolf Optimization Adaptive Formation method envisions the optimum course. An ideal route is then selected from the known routes to secure the techniques of data key management; Homomorphic Encryption is used here. In terms of criteria such as end-to-end latency, packet distribution ratio etc., the productivity in the functioning of the expected methodology is measured.

In MANETs with congestion perception, Reddy, A. P., & Satyanarayana, N. [12] suggest a method known as reliable and secure multipath routing. Bandwidth is the goal of this strategy, and latency is taken into consideration while routing. In this method, the residual energy and reliability of the connections in the network are estimated by the network. It also calls the receiving energy and the transmission energy of the node when calculating the residual energy. The stability of the LET connection is then calculated; this LET is obtained using motion parameters (i.e., velocity, direction of the nodes). The network chooses the route to relay the data packets between the nodes depending on these criteria.

Banoth Rajkumar, Gugulothu Narsimha [13] suggests safe multi-path routing and data transfer where RREQ packets are signed for route discovery using digital signatures. As the destination collects the first RREQ packets from the server, all signatures are checked by the destination and the path list is cached by the source node session key. Then, it sends the RREP to the source node using the same direction. If the signature has been checked, the route is approved. The message components are encrypted at the source node using session keys and the hash function. Safe routing may be achieved depending on the confidence level of the nodes. To select an optimum safe routing route, an algorithm was used. The messages are then split into four bits, gently encrypted, and XOR operations are conducted. Lastly, the target node decrypts the initial message and restores it.

G. V. Madhu Viswanatham, S. G. N. Anjaneyulu and B. Venkateswarlu [14] The key emphasis of this paper is on authentication and secrecy during data transfer between MANET nodes. To provide security and strengthen data protection, we suggested a novel solution. A transmitting signature scheme built to use the issue of polynomial symmetrical decomposition dependent on non-commutative division seedlings. The principle is to combine the framework of signatures and multipath routing. And if an intruder happens to get one or more transmitted pieces, the likelihood of restoration of the original message is almost zero.Dr. D. Jagadeesan, G. Asha, M. Geetha, Dr. S.K. Srivatsa[15] Multipath routing is a commonly employed method in the Mobile Ad Hoc Networks for utilizing many alternate routes (MANETs). Message transmission in multipath routing is split into streams and is transmitted along different routes. There could be a risk of loss in the direction during the delivery of the packet. In order to resolve this setback, an alternate route must be chosen to effectively send the message stream. Based on the latest ERS (Effective Route Selection) criterion, which requires maximum usable bandwidth and minimal transmitting period, the efficient alternate path is chosen. The proposed parameter is introduced in the Network Simulator (NS-2) and is evaluated for performance. The new ERS parameter selects an effective, bandwidth-increased alternative route and increases network efficiency.

III.THE PROPOSED METHOD OF EFFICIENT ROUTING

Efficient routing [16-25]in MANETs ensures that the effectively transmitted the data from source to destination and decreases the info loss occurring throughout the transmission. Furthermore, to decrease the energy loss during transmission and boost the duration of this system, the paper presents the hybrid algorithm employing the CSO along with SSA algorithms. There are two main steps: the first is fuzzy clustering and CH selection utilizing maximum values of direct, indirect, and recent confidence; the second is intruded node identification using a predefined threshold value of 0.5J; if the trust value of any node exceeds the predefined threshold value, it is considered a regular node; otherwise, it is considered an intruded node. We prevent the intruded node in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3108807, IEEE Access

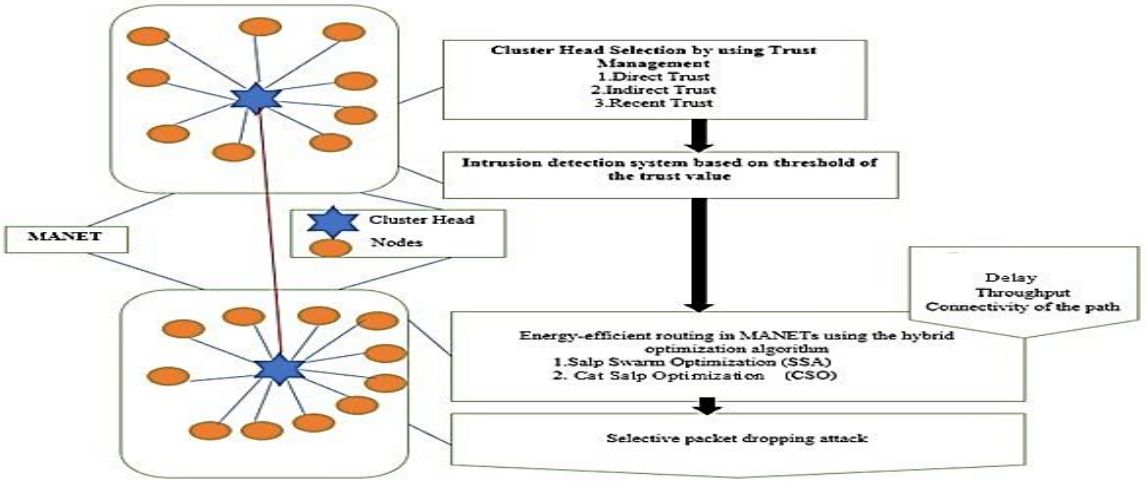

FIGURE 1. **Proposed Trust aware secure energy-efficient Hybrid Routing protocol**

this way for safe data transfer from source to destination. The best paths are then picked using the proposed hybrid C-SSA algorithm, which is based on the planned objective feature and takes into account the capacity, throughput, and communication of the path. The hybrid optimization-based trust conscious safe energy efficient routing in MANETs as seen in Figure 1.

A. TRUST MANAGEMENT SYSTEM

1) DIRECT TRUST (DT):

The DT is predicated on the approximate period of communicating between i^{th} node and d^{th} destination n. DT is quantified as the gap on the list of actual and the projected period of i^{th} node to authenticate the public key written by the d^{th} destination. So, DT involving i^{th} node and d^{th} destination has been represented as,

$$DT_i^d(\tau)=\frac{1}{3}\left[DT_i^d(\tau-1)-\left(\frac{\tau_{appx}-\tau_{est}}{\tau_{appx}}\right)+\omega\right] \quad (1)$$

Where, τ_{appx} describes the approximate period and τ_{est} defines the expected period for authenticating the public key. To put it differently, τ_{appx} and τ_{est} are the estimated period for receiving and sending the public key by the destination and also the node. ω Signifies the opinion variable of these nodes.

2) INDIRECT TRUST (IDT):

The node with the opinion variable is plotted predicated on DT. But node with no witness variable is authenticated with the IDT, that is given by,

$$IDT_i^d(\tau)=\frac{1}{r}\sum_{i=1}^{r}DT_i^d(d) \quad (2)$$

where, r Specifies the overall neighbours of this node i.

3) RECENT TRUST (RT):

Recent trust is calculated with the DT and also IDT alongside the crucial validity and the admitting the destination or sink, that will be presented in part of their moment. The RT is devised as,

$$RT_i^d(\tau)=\alpha*DT_i^d(\tau)+(1-\alpha)*IDT_i^d(\tau) \quad (3)$$

Where, $\alpha=0.3$

B) CH CHOICE DEPENDING ON THE FUZZY CLUSTERING STRATEGY

Fuzzy Clustering is a clustering process in which the patient nodes belonging to a cluster are assigned to a level depending on the membership level. The most critical aim of fuzzy clustering is to determine the best cluster head based on the highest level of node confidence. The best cluster head is returned to the node that earns the maximum benefit of this confidence. The drawbacks of utilizing the Fuzzy Clustering Theory are the assumption that the technique functions well with the overlapped numbers and that the patient data point is one of a variety of cluster centers as a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3108807, IEEE Access

consequence of this membership. The function of fuzzy clustering is one of minimization. This is mentioned as,

$$J_f = \sum_{i=1}^{r}\sum_{j=1}^{m} u_{ij}^{f} \times \left\| n_i - H_j \right\|^2 ; 1 \le f \le \infty \qquad (4)$$

Where, n_i suggests the i^{th} node from the MANET, H_j signifies that the j^{th} cluster head, also signifies the Euclidean distance between your i^{th} node and the j^{th} cluster head. The fuzziness indicator is given as, $\{f | f \in Q > 1\}$. The purpose function is notated as, J_f also f defines the fuzzifier. The nodes which display minimal Euclidean distance in regard to the cluster head is delegated beneath a cluster head set in a cluster. The term for a node to become a CH is founded max values of direct, indirect, and recent trust, the maximization function(M), which is given as,

$$M=\frac{1}{3}\{D + I + R\} \qquad (5)$$

Where D, I and R are direct, indirect, and recent trust values. The values of the D,I and R calculated by using equations (1)(2) and (3)

C) THRESHOLD VALUE COMPARISON FOR IDENTIFYING THE INTRUDED NODES

After the best CHs are calculated, then the system intrusion is calculated based upon the optimism facets of these nodes from the system [26-30], which is worth noting that landlords have been characterized with the sink node working with the comprehension delivered into the spout through the CHs from the nodes (or cluster associates). If the attacker has been identified, the intruder node is barred from communicating with the rest of the network. Predefined threshold value (0.5J) for predicting intruders in the sink node. The administrator may nevertheless set the threshold value according to needs. Usually, the threshold value is 0.5J. The remaining energy range of a specific node helps us determine a channel's transmission power and connection condition. For example, if the energy of a node is low, the probability of connecting to a distant next node may be lower and thus the node is not part of a reliability pair. On the other hand, if the energy of the node is high, the transmission power of a node may be raised to cover far nodes. The key goal of intrusion detection is to ensure secure network connectivity with minimal energy consumption and transmission delay.

D) EFFECTIVE ROUTING WITH A HYBRID ALGORITHM

Even the Hybrid optimization algorithm establishes the most useful jumps for MANET routing development. The proposed algorithm purpose is to function can be utilized to decide on the very best hopes for routing.

1) RESOLUTION CONVERTING

Even the requirement for immediate answer programming will signify the remedy of the Optimization algorithm, and also the remedy is just the avenues chosen for its navigation in MANETs. The maximal confidence equation (5) represents the CHs that are selected to promote efficient routing [31-39] from the device by reducing data loss during transmission. For the least amount of energy waste, the routing latency is reduced.

2) DESIGN OF THE OBJECTIVE

The sum of energy left in the nodes, the path's throughput, and the path's accessibility decide the path's health. As a consequence, the fitness function, denoted by, is a maximization function.

$$F=\frac{1}{3}\{e + t + c\} \qquad (6)$$

Where e represents energy, t represents throughput and c means connectivity of the path and are calculated using the nodes in the path. Equations are used to calculate the energy left in the node

$$E^{remain}(\tau) = E^{remain}(\tau) - E^{transmit}(\tau - 1, \tau) - E^{recieve}(\tau - 1, \tau) \qquad (7)$$

Where, E^{remain}, $E^{transmit}$ and $E^{recieve}$ are the remaining and required energy for communicating a single bit of information. Throughput is calculated because the proportion of overall Pieces sent across the system per minute by way of a management, also can be Expressed as,

$$u = \frac{\upsilon}{\tau} \text{ bps} \qquad (8)$$

Where, υ implies no of transmitted bits from source to destination and τ defines the time in seconds. The connectivity has been developed on bidirectional connections between two nodes, that can be written,

$$y = \frac{1}{g}\left[\sum_{i=1}^{g} \frac{y_i}{cc} .\right] \qquad (9)$$

Where, y_i implies the connectivity of i^{th} node, and cc represents overall contacts.

E) HYBRID (SSA AND CSO) OPTIMIZATION ALGORITHM

The CSO method is paired with the traditional SSA algorithm in the hybrid optimization. Through keeping a good compromise between the extraction and exploration phases, the proposed mixture optimization process incorporates the advantages of both algorithms to achieve the overall optimum resolution. The recommended algorithm is simple to execute and has an adaptively updating control restriction. As a result, the hybrid algorithm's primary aim is to solve the problems associated with the conventional SSA method by integrating CSO. The proposed algorithm will probably reach worldwide optimum outcomes for uni-modal, multi-modal, and mix outcomes. SSA relies upon the swarm behavior of those salp chain, also is intended to fix real world problems. The SSA is nominated properly for just two classes of salps, pioneer and supporter. The main salp contributes the salp series, which is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3108807, IEEE Access

subsequently followed closely with another salps. The admirer salp updates its role based on the leader's location, while the chief salp updates its place centered on the path of the food supply. The following are the basic SSA equality principles:

$$X^{j}_{t+1} = 1/2 \times [X^{j}_{t} + X_t^{j-1}], \quad (10)$$

At which X^{j}_{t} refers into this standing of this j^{th} salp or pioneer in iteration and X_t^{j-1}signifies the standing of this $(j-1)^{th}$ salp in iteration t. X^{j}_{t+1}signifies the standing of this j^{th} salp in iteration (t+1). Likewise, the Conventional formula of this CSO algorithm is provided as

$$X_{t+1} = (1 \pm D \times r) \times X_t \quad , \quad (11)$$

At which X_{t+1} refers into this newest place of your cat, X_t signifies the prior spot of their cat. r indicates that the arbitrary number carrying the worth [0,1] D also D stipulates the utmost girth one of the older and the brand-new rankings from the chosen measurement. Even the CSO algorithm advances the optimization with two manners, namely, both tracing and hunting manners. From the hunting style, the cats break, whilst at the carrying out mode, the cats pursue their prey. The hunting and tracing styles permit the collection of the international best option. So, in summary, an individual could express the cats focus from the hunting style, and thus the cats at the snore are significantly somewhat less. The Conventional formula of CSO is granted as

$$X^{j}_{t+1} = X^{j}_{t} + \upsilon^{j}_{t+1}, \quad (12)$$

At which X^{j}_{t+1} refers into this newest placement of j^{th} cat and X^{j}_{t} defines that the positioning of j^{th} cat inside the past iteration. υ^{j}_{t+1} defines the speed of this j^{th} cat at the $(t+1)^{th}$ iteration. The speed is substituted from the Aforementioned equation, and this can be granted as

$$X^{j}_{t+1} = X^{j}_{t} + \upsilon^{j}_{t} t + r_1 \times \gamma_1 (X_{best} - X^{j}_{t}), \quad (13)$$

In which $\gamma 1$ suggests that the continuous and r1 is that the arbitrary number in [0,1]. Re Arranging the equations, we receive

$$X^{j}_{t} = 1/(1-r1 \times \gamma 1) \, [\, X^{j}_{t+1} - \upsilon^{j}_{t} - r1 \times \gamma 1 \times X_{best} \,] \quad (14)$$

F) DERIVING THE UPGRADE FORMULA OF THE SUGGESTED C-SSA ALGORITHM

Even the modified upgrade equation is based via the substitution of this upgrade equation of CSO from the conventional formula of SSA awarded as

$$X^{j}_{t+1} = \frac{(1-r1\times\gamma 1)}{1-2r1\times\gamma 1)} \times \left[X_t^{j-1} - \frac{\upsilon^{j} + r1\times\gamma 1\times X_{best}}{1-r1\times\gamma 1} \right] \quad (15)$$

In the suggested equation, it's apparent the job of this salp from the present iteration is upgraded dependent upon the optimal location of this salp, location of their salp inside the prior iteration, arbitrary variety, and the speed of this salp.

Algorithmic stages of the proposed cat slap single-player algorithm (C-SSA)

The steps of the proposed algorithm are set out as follows in determining the optimal hop path:

a) Initialization: As the first stage, the salp chain population is initialized

$$X\, j; (1 \leq j \leq m) \quad (16)$$

Where m refers to the salp chain overall salps and Xj refers to the jth salp location.

b) Fitness evaluation: The fitness of the salp is assessed on the basis of the equation 6 to resolve the maximizing problem. The fitness of all search rooms is evaluated and the salp matching maximum fitness is selected as the best search agency on which the leader updates the position.

c) Determine the best search agent: the greatest fitness search agent is referred to as the best search agent for the leader salp location upgrade.

d) Update the leading salp position: The location of a salp is calculated on the basis of the following formula after the optimal search agent is identified:

$$X_j^{lead} = \begin{matrix} X_{best} + \rho_1 ((u_j - l_j)\rho 2 + l_j); \rho 3 \geq 0 \\ X_{best} - \rho_1 ((u_j - l_j)\rho 2 + l_j); \rho 3 < 0 \end{matrix} \quad (17)$$

Where X_j^{lead} refers to the lead salp location and X_{best} indicates the food source position. The random numbers are referred to as ρ1, ρ2, and ρ3, and uj and lj refer to the upper and lower limits. The random number ρ1 is important because it is necessary to balance the exploration and exploitation phases well.

$$\rho 1 = 2e^{-(4t/t_{max})^2} \quad (18)$$

When t refers to iteration, then the maximum iteration number is indicated by t_{max}. The two random numbers, ρ2 and ρ3, acquire the value from 0 to 1, and indicate whether the location of the salp is towards the positive or negative infinity.

e) Update the position of the supporters: Once the leader salp updates his position, his position is updated depending on the leader's position. The typical position update equation for the following is based on Newton's motion law, which is changed with the update CSO equation. The follower's location is therefore updated based on Equation 15.

f) Update the upper and lower limits of the variables: The top and bottom boundary of uj and lj are changed to move the next iteration in search of the best manager at the conclusion of the position update.

g) Terminate: Steps from b) to f) are repeated until the optimal solution can be found for the maximum iterations.

IV RESULTS

Even the section discusses the link between the productive routing depending about the C-SSA algorithm together side all the comparative investigation predicated on the functionality metrics to show the efficacy of this suggested procedure.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3108807, IEEE Access

A) INVESTIGATIONAL ARRANGEMENT

The simulator has been used from the NS-2 [26] instrument, and also the simulator has been improved with one 100 nodes at the simulation atmosphere. Here in simulation results we are taking simulation time as 40mse

B) PERFORMANCE METRICS

Delay, energy, throughput and detection rate are the parameters used in the study, and the proposed protocol is compared to all existing procedures that are based on competence metrics with and without attack. The apparatus energy would be that the energy which remains from the nodes following the transmission is now stopped, also it ought to be described as a max worth to delegate the device's period. The outcome signal of this system is related for the accumulative amount of information delivered via the system in a specific time framework, whereas the interval denotes the full time that it can take with this particular information to be transmitted.

C) RELATIVE TECHNIQUES

The techniques used for the contrast include Energy Aware on Demand Routing Protocol (EA-DRP) (7), Energy Efficient Optimized Hierarchical Routing Algorithm (EE-OHRA) route (8) are used to compare with the proposed trust-based energy-efficient hybrid routing algorithm.

1) COMPARATIVE EVALUATION OF THE SUGGESTED METHOD

DELAY

In following figures, the comparative evaluation of the recommended method. Figure 2 shows the relative assessment centred on delay. When the simulation time is 40 secs, the delay of the methods, EA-DRP, Energy Efficient EE-OHRA route, and proposed trust-based energy-efficient hybrid routing algorithm is 0.007, 0.004 and 0.003 m sec, respectively.

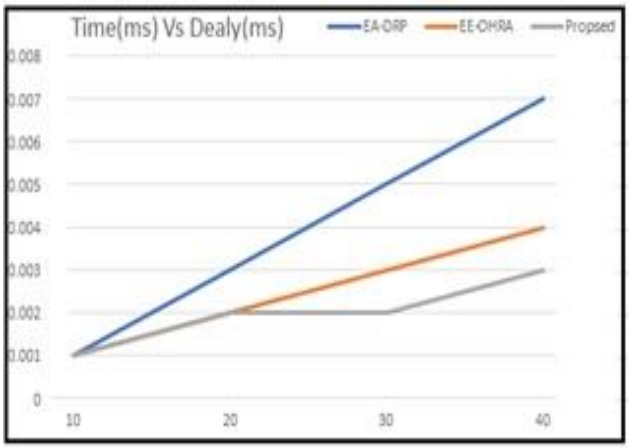

FIGURE 2. Delay of the Proposed method

From the simulation outcomes it reveals that suggested trust-based energy-efficient hybrid routing algorithm acquired a minimum delay of 0.005 msec when compared with existing two techniques of EA-DRP and Energy Efficient EE-OHRA methods.

ENERGY CONSUMPTION

Figure 3 shows the relative analysis cantered on energy expenditure. When the energy consumption at 40 secs time is, EA-DRP, Energy Efficient EE-OHRA route, and proposed trust-based energy-efficient hybrid routing algorithm is 0.24, 0.22 and 0.11 m Joules, respectively.

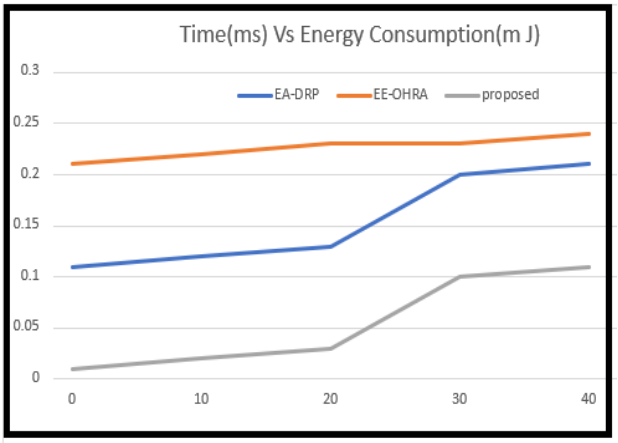

FIGURE 3. Energy consumption of the Proposed Method

From the simulation solutions it indicates that recommended trust-based energy-efficient hybrid routing algorithm acquired a minimum energy consumption of 0.11m joules when compared with existing two techniques of EA-DRP and Energy Efficient EE-OHRA methods.

THROUGHPUT

Figure 4 shows that the relative investigation established on throughput. After the delay is 40 secs, the throughput of those approaches, EA-DRP, Energy Efficient EE-OHRA route, and proposed trust-based energy-efficient hybrid routing algorithm is 0.64, 0.45, and 0.74 bps, respectively.

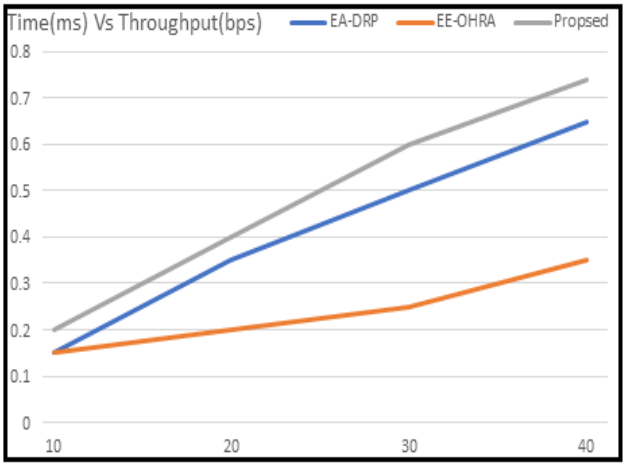

FIGURE 4. Throughput of the Proposed Method

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3108807, IEEE Access

From the simulation outcomes it indicates that suggested trust-based energy-effective hybrid forwarding algorithm acquired a maximum Throughput of 0.74 bps when compared with existing two techniques of EA-DRP and Energy Efficient EE-OHRA methods.

DETECTION RATE

Figure 5 displays the results of a comparison based on detection rate. When the delay reaches 40 seconds, the techniques' detection rates are, EA-DRP, Energy Efficient EE-OHRA route, and proposed trust-based energy-efficient hybrid routing algorithm is 80, 75, and 90 %, respectively

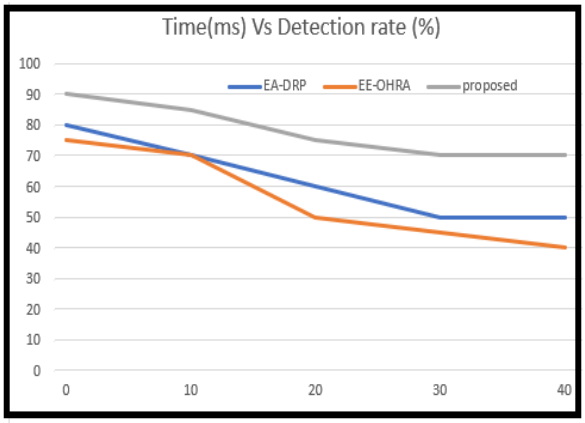

FIGURE 5. Detection rate of the Proposed Method

According on the simulation findings, the suggested trust-based energy-efficient hybrid routing algorithm
acquired a maximumdetection rate of 90% when compared with existing two techniques of EA-DRP and Energy Efficient EE-OHRA methods.

4.4 COMPARATIVE INVESTIGATION FROM THE EXISTENCE OF THE SELECTIVE FORWARDING ASSAULTS GRAPHICS

The relative examination of the method indicated in the following data. The relative delay estimate is shown in Figure 6 (a). The EA-DRP latency, the Energy Efficient EE-OHRA route and the proposed secure trust-based energy efficient hybrid router algorithm, respectively, is 0.008 0.007 and 0.006 m sec, with a period of 40 seconds. The relative energy expenditure study as shown in Figure 6 (b). EA-DRP energy intake, the Energy Efficient EE-OHRA route, and the proposed secure confidence-based hybrid routing algorithm, respectively, at 0.25, 0.23 and 0.10 m Joules, is 40 seconds in length. The relative performance-based research is presented in Figure 6 (c). The EA-DRP, Energy Efficient EE-OHRA and suggested secure energy-sensitive hybrid routing algorithm, after a 40 second delay, is 0.65, 0.70, and 0.76 bps, respectively. The comparison with the detection rate is shown in Figure 6 (d). EA-DRP detection rates, the Energy Efficiency EE-OHRA route and the proposed secure energy efficient hybrid routing algorithm based on trust are 79, 74 and 89 per cent, when the delay is 40 seconds. correspondingly. From the above results it is observed that proposed method showing better results when compared to existing techniques in the presence and absent of the selective packet dropping attack.

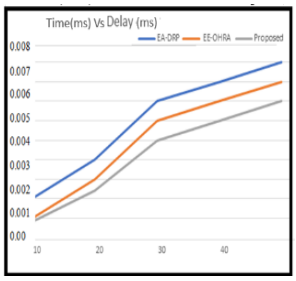

FIGURE 6(a). Delay

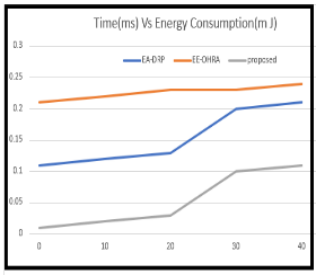

FIGURE6(b). Energy consumption

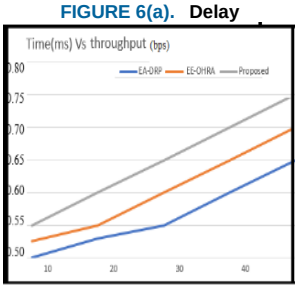

FIGURE6(c). Throughput

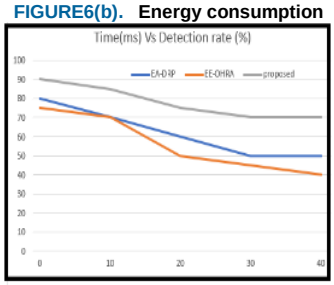

FIGURE 6(d). Detection rate

V CONCLUSION

The research community has garnered great attention from mobile ad hoc networks owing to its prospective uses. The intrinsic features of these networks nevertheless render them susceptible to a broad range of assaults. The energy and security of these wireless networks is still a major obstacle to broad deployment. Both the energy crisis and security issues are resolved by the secure energy-efficient routing protocol. A successful routing approach was made employing the cat along with salp swarm optimization calculations. At Step One, the CHs are Determined Utilizing the Fuzzy clustering algorithm together with utmost trust values for direct, indirect, and recent trust. And, depending on the predefined threshold value, intruded nodes are observed. The CHs are in charge of routing data packets to the drain, which are effectively routed over several hops. In MANET, but the most useful leaps for innovative routing have been selected with a hybrid optimization called C-SSA optimization," that unites CSO along with SSA. The suggested algorithm includes a much high convergence speed, and also the hybrid vehicle focuses on storage, throughput, along with route link limitations. With 100 nodes, the proposed method obtained a minimal energy of 0.11m joules, a negligible latency of 0.005 msec, a maximum throughput of 0.74 bps, a maximum packet delivery ratio of 0.99 percent, and a maximum detection rate of 90%. Similarly, as contrasted to current approaches, the proposed approach produced reasonable results for the selective packet dropping attack. The future work needs to analysis the performance of the proposed system by applying the more no of security attacks.

REFERENCES

[1] Neenavath Veeraiah, B. Tirumala Krishna "Trust-aware Fuzzy Clus-Fuzzy NB: intrusion detection scheme based on fuzzy clustering and Bayesian rule"Springer, Wireless Networks 25, 4021–4035 (2019), DOI:10.1007/s11276-018-01933-0,

[2] Neenavath Veeraiah, B. Tirumala Krishna "A Comparative analysis of Energy Efficient Multipath Routing in MANET"Jour of Adv Research in Dynamical & Control Systems, Vol. 12, No. 3, 2020,

[3] Neenavath Veeraiah, B. Tirumala Krishna "A Fuzzy Clustering with Optimized Cluster Head Selection Method in MANET"International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-2, July 2019.

[4] A. F. Subahi, Y. Alotaibi, O. I. Khalaf and F. Ajesh, "Packet drop battling mechanism for energy aware detection in wireless networks," *Computers, Materials & Continua*, vol. 66, no.2, pp. 2077–2086, 2021.

[5] Khalaf, O. I., Abdulsahib, G. M., & Sabbar, B. M. (2020). Optimization of Wireless Sensor Network Coverage using the Bee Algorithm. J. Inf. Sci. Eng., 36(2), 377-386..

[6] Veeraiah, N., Krishna, B.T. "An approach for optimal-secure multi-path routing and intrusion detection in MANET",Evol. Intel. (2020).

[7] Prasad P, R, Shankar, S. Efficient Performance Analysis of Energy Aware on Demand Routing Protocol in Mobile Ad-Hoc Network. *Engineering Reports*. 2020; 2:e12116.

[8] S. Vinod Kumar, Dr. V. AnurathaEnergy. Efficient Routing For Manet Using Optimized Hierarchical Routing Algorithm (Ee-Ohra). International Journal of Scientific & Technology Research VOLUME 9, ISSUE 02, FEBRUARY 2020

[9] Borkar, G.M., Mahajan, A.R. "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", Wireless Netw**23,** 2455–2472 (2017).

[10] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq and T. Saba, "Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function", in IEEE Access, vol. 5, pp. 10369-10381, 2017.

[11] Kavuru Tejaswi Uttej Kumar Nannapanenia, Dr. U. Srilakshmi, Alaparthi Sravyaa "Cluster-Based Collection point Energy Efficient Routing Protocol for the Mobile Sink in Wireless Sensor Network" International Journal of Grid and Distributed Computing 2020, Volume 13,Issue 2,Pages 787 – 796.

[12] MallikarjunaAnantapur,VenkanagoudaChanabasavanagouda Patil "Position Update Secure Routing protocol for MANET",International Journal of Intelligent Engineering and Systems, Vol.14, No.1, 2021.

[13] Rajashanthi, M., Valarmathi, K. "A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs",Wireless Pers Commun**112,** 75–90 (2020).

[14] Reddy, A. P., & Satyanarayana, N. (2017). "Energy-efficient stable multipath routing in MANET. Wireless Networks",23(7), 2083–2091.

[15] Banoth Rajkumar,Gugulothu Narsimha "Secure multipath routing and data transmission in MANET",Int. J. Networking and Virtual Organisations, Vol. 16, No. 3, 2016.

[16] G. S. G. N. Anjaneyulu, V. Madhu Viswanatham and B. Venkateswarlu "Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks",Advances in Applied Science Research, 2011, 2 (4):177-186.

[17] Dr. D. Jagadeesan, G. Asha, M. Geetha, Dr. S.K. Srivatsa "Effective Route Selection Based on Transmission Time and Bandwidth for Multipath Routing in MANETs",International Journal of Computer & Organization Trends –Volume 5 Issue 2 March to April 2015.

[18] 13. Li J, Lewis HW (2016) "Fuzzy clustering algorithms – review of the applications" In: Proceedings of the IEEE international conference on smart cloud (SmartCloud), pp 282–288.

[19] Wang N-C, Su Y-L. A power-aware multicast routing protocol for mobile ad hoc networks with mobility prediction. Wireless Pers Commun. 2005;43:1479-1497.

[20] Vazifehdan J, Venkatesha Prasad R, Onur E, Niemegeers I. Energy-aware routing algorithms for wireless ad hoc networks with heterogeneous power supplies. ComputNetw. 2011;55:3256-3274.

[21] Uppalapati, S. (2020). Energy-efficient heterogeneous optimization routing protocol for wireless sensor network. Instrumentation Meuser Métrologie, Vol. 19, No. 5, pp. 391-397. https://doi.org/10.18280/i2m.190510

[22] Khalaf, O. I., Abdulsahib, G. M., Kasmaei, H. D., & Ogudo, K. A. (2020). A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications. International Journal of eCollaboration (IJeC), 16(1), 16-32..

[23] Nithya V, Ramachandran B, Vaishanavi Devi G. Energy efficient tree routing protocol fortopology controlled wireless sensor networks. Int J Commun Antenna Propag. 2015;5:1.

[24] Parthiban P, Sundararaj G, Maniiarasan P. Maximizing the network life time based on energy efficient routing in ad hoc networks. Wireless Pers Commun. 2018;101:1143-1155.

[25] Khalaf, O. I., & Sabbar, B. M. (2019). An overview on wireless sensor networks and finding optimal location of nodes. Periodicals of Engineering and Natural Sciences, 7(3), 1096-1101.

[26] Khalaf, Osamah Ibrahim, and Ghaida Muttashar Abdulsahib. "Energy Efficient Routing and Reliable Data Transmission Protocol in WSN." *Int. J. Advance Soft Compu. Appl* 12, no. 3 (2020).

[27] Abdulsaheb, G. M., Khalaf, O. I., Sulaiman, N., Zmezm, H. F., & Zmezm, H. Improving Ad Hoc Network Performance by using an Efficient Cluster Based Routing Algorithm.

[28] Dinesh Chander, Rajneesh Kumar,QoS Enabled Cross-Layer Multicast Routing over Mobile Ad Hoc Networks,Procedia Computer Science,Volume 125,2018,Pages 215-227,ISSN 1877-0509.

[29] Wang N-C, Su Y-L. A power-aware multicast routing protocol for mobile ad hoc networks with mobility prediction. Wireless Pers Commun. 2005;43:1479-1497.

[30] Vazifehdan J, Venkatesha Prasad R, Onur E, Niemegeers I. Energy-aware routing algorithms for wireless ad hoc networks with heterogeneous power supplies. Comput Netw. 2011;55:3256-3274.

[31] Jinhui S, Harms J. Position-based routing with a power-aware weighted forwarding function in MANETs. Paper presented at: IEEE International Conference on Performance, Computing, and Communications; 2004. https://doi.org/10.1109/pccc.2004.1395026.

[32] Floriano De Rango, Fotino M, Marano S. EE-OLSR: energy efficient OLSR routing protocol for mobile ad-hoc networks. Paper presented at: MILCOM 2008–2008 IEEE Military Communications Conference; 2008. https://doi.org/10.1109/milcom.2008.4753611.

[33] Nithya V, Ramachandran B, Vaishanavi Devi G. Energy efficient tree routing protocol for topology controlled wireless sensor networks. Int J Commun Antenna Propag. 2015;5:1.

[34] Parthiban P, Sundararaj G, Maniiarasan P. Maximizing the network life time based on energy efficient routing in ad hoc networks. Wireless Pers Commun. 2018;101:1143-1155.

[35] Shivashankar, Varaprasad G, Narayanagowda SH. Implementing a new power aware routing algorithm based on existing dynamic source routing protocol for mobile ad hoc networks. IET Netw. 2014;3:137-142.

[36] Loo J, Lloret Mauri J, Ortiz J(Eds.). Mobile Ad Hoc Networks. Boca Raton: CRC Press; 2012. https://doi.org/10.1201/b11447.
[37] Santhi G. Nachiappan A. Agent based adaptive multicast routing with QoS guarantees in MANETs. 2010 Second International conference on Computing, Communication and Networking Technologies, Karur; 2010;1-7. https://doi.org/10.1109/ICCCNT.2010.5591721.
[38] Rajendra PP, Shankar. Improvement of battery lifetime of mobility devices using efficient routing algorithm. Asian J Eng Technol Appl. 2017;1:13-20.
[39] Venkanna U, Agarwal JK, Velusamy RL. A cooperative routing for MANET based on distributed trust and energy management. Wireless Pers Commun. 2015;81:961-979. https://doi.org/10.1007/s11277-014-2165-5.

NEENAVATH VEERAIAH (born on 18th May 1986) is an Indian academician. He is having 12 years of teaching experience. He received his B. Tech degree from Gudlavalleru engineering college, gudlavalleru in the year 2007. M. Tech degree from Lakkereddy Balireddy college of engineering, mylavaram in the year 2011.Now he is pursuing his Ph. D in communication & signal processing at JNTUK University, Kakinada, A.P, India. He got amount of 7 lacks rupees of fund from Indian government one of the leading funding organization department of science & technology (DST). He published 18 international research papers over the years as well as attended a greater number of workshops and IEEE conference. He is also a member of several professional, scientific organizations.

OSAMAH IBRAHIM KHALAF is Senior Engineering and Telecommunications Lecturer in Al-Nahrain University. He has hold 17 years of university-level teaching experience in computer science and network technology and has a strong CV about research activities in computer science and information technology projects. He has had many published articles indexed in (ISI/Thomson Reuters) and has also participated and presented at numerous international conferences. He has a patent and has received several medals and awards due to his innovative work and research activities. He has good skills in software engineering including experience with: .Net, SQL development, database management, mobile applications design, mobile techniques, Java development, android development, and IOS mobile development, Cloud system and computations, website design. I am Editor in Chef and main guest editor in many Scopus and SCI index journals His brilliant personal Strengths are in highly self-motivated team player who can work independently with minimum supervision, strong leadership skills, and outgoing personality. He got his B.Sc. in software engineering field from Al_Rafidain University College in Iraq. Then he got his M. Sc. in computer engineering field from Belarussian National Technical University. After that, he got his PhD in the field of computer networks from faculty of computer systems & software engineering -University Malaysia, Pahang. He has overseas Work experiences in University in Binary University in Malaysia and University Malaysia Pahang.

C.VP.R.Prasad is the Professor and Head of, Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Hyderabad. He received his M.Tech., from Acharya Nagarjuna University in the year 2010. He received his Ph.D. from Acharya Nagarjuna University in the year 2015. He has 22 years of Academic and 13 years of Research Experience. His main research areas are Knowledge Engineering, Agile Processing, and Artificial Intelligence & Machine Learning. He has published Thirty-Five (35) research papers in Scopus Journals. He has published two (2) SCI papers. Currently, he is acting as a research supervisor at Acharya Nagarjuna University and KL University. Under his guidance One (1) Scholar was successfully awarded a Ph.D. degree from Acharya Nagarjuna University. He published Four (4) patents. He was acted as a convenor for international conferences, Workshops, FDPs at Malla Reddy Engineering College for Women. He is a life member of ACM, ISTE, and CSI. He has done various online courses in NPTEL, COURSERA, and COGNITIVE.AI. He has actively participated in several workshops, seminars, and Faculty Development Programs. He received the award of best academic leader from I2OR. He acted as a reviewer for inderscience and Allied Academies Journals. He received a grant from AICTE

YOUSEEF ALOTAIBi is an Associate Professor in the Department of Computer Science, College of Computer and Information Systems, at Umm Al-Qura University, Saudi Arabia. He completed his PhD from the Department of Computer Science and Computer Engineering, La Trobe University in, Melbourne – Australia in 2014. He received his Master in Information Technology (Computer Network) from La Trobe University in 2009. He has published several international Journal and Conference papers. His research interests include business process modelling, business process reengineering, information system, security, business and IT alignment, software engineering, system analysis and design, sustainability and smart cities development.

ABDULMAJEED ALSUFYANI. Abdulmajeed Alsufyani received the bachelor's degree (Hons.) in computer science from Taif University, Saudi Arabia, in 2006, and the master's degree in Computer Science and the Ph.D. degree in computer science from the University of Kent, U.K., in 2010 and 2015, respectively. He is currently an Associate Professor of Computer Science at the College of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include Computational Intelligence, Computational Neuroscience, Machine Learning Algorithms.

SALEH AHMED ALGHAMDI received the Bachelor of Education degree (Hons.) from the Department of Computer Science, Teachers College, Riyadh, Saudi Arabia, in 2004, the Master of Information Technology degree from La Trobe University, Melbourne, Australia, in 2010, and the Doctor of Philosophy degree in computer science from the Royal Melbourne Institute of Technology (RMIT) University, Melbourne, in 2014, thesis title A Context-aware Navigational Autonomy Aid for the Blind. He is currently an Associate Professor with the Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia. His research interests include context awareness, positioning and navigation, and visually impaired assistance.

NAWAL ALSUFYANI received the B.Sc. degree in Computer Science from Taif University, KSA, in 2009, and the M.Sc. degree in Information Security and Biometrics from the University of Kent, UK, in 2014. She obtained her Ph.D. degree in Electronics Engineering with the University of Kent, UK in 2019. She is currently an Assistant Professor of Computer Science at the College of Computers and Information Technology, Taif University. Her research interest focuses on Biometrics, Computer Vision, Pattern Recognition, and Machine Learning Algorithms.